ANTI-MONEY LAUNDERING AND TERRORISM FINANCING COMPLIANCE PROGRAM

Table of Contents

Part A. Background information
1. Background information

This document confirms CruisePay’s commitment to preventing money laundering and financing of criminal activity in its business practices and transactions. The following section sets forth a high-level summary of AML/TF risks and the company's obligations under the law.

Canada is an active participant in the prevention of financial crime conducting efforts through a comprehensive set of laws and regulations, particularly a national piece of legislation called the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and the applicable laws.

1.1 Overview of money laundering
Money laundering is a predictable offense that means the process of turning illegally-gained profits into legal. It typically follows a basic three-step process: placement, layering and integration. Firstly, the non-legitimate profits are furtively placed into the economy. Then, they are given another form to create confusion by establishing multiple layers of transactions to hide their origin and ownership. Finally, they are placed back into the economy through extra transactions until they appear "clean."

1.2 What is Terrorist Financing?
Terrorist financing is clearly defined in Canadian law. If a company or person knowingly or unknowingly sends money or lends property to terrorists, they are already funding their actions. There is a specific purpose for terrorist activity: intimidation of the population. It may also be a desire to apply by order to the government.

Terrorists need financial support. Otherwise, they will not be able to continue their activities and achieve their goals. Some organizations receive funds through third-party money laundering. They disguise transactions as receipts from a source that cannot be traced back.

Terrorist financing methods

There are two sources of terrorism financing:

- receiving money from a country government, organization or individual;
- engaging in activities that can be legal and criminal.

Most often, terrorist groups are involved in smuggling, fraud, and drug trafficking. But sometimes they open legitimate companies and use the resulting profits to finance their illegal activities. It also can have charitable status and sale of seats for seminars, various events. People believe that they give finance for good deeds.

Terrorist organizations use almost the same methods as criminal groups. Therefore, terrorist financing is very similar to money laundering. To stop this direction and track the financial activities of the organization, it is necessary to fight these criminal areas.

1.3 Our responsibilities
Money Services Businesses (MSBs) in Canada are reportable to the government. By law, they:

1. Create special compliance programs in order to provide reports at the right time, maintain documentation and identify customers correctly.
2. Maintain records of transactions and customer identities.

3. Provides FINTRAC data on suspicious transactions or large money transfers.

There is a compliance program for each of the financial companies required by the law. All firms must:

- hire a specialist who will monitor their compliance with all legal requirements;
- develop a written policy for the operation of the company;
- record possible risks and suspicious transactions during which there is a possibility of money laundering;
- draw up a plan for the person to act on behalf of the company;
- conduct risk assessments and check their effectiveness every 2 years or more often.

1.4 Penalties for non-compliance

FINTRAC can impose AMP3 (administrative fine) on companies that do not comply with legal requirements.

The violation is considered minor, serious, or very serious. Therefore, the punishment is also different:

• 1 - 1000 Canadian dollars (CAD);

• 1 - 100,000 Canadian dollars;

• 1 - 100,000 Canadian dollars (for an individual) and 1 - 500,000 Canadian dollars (for a legal entity).

Fines can be applied to every violation of the law. If there are several, the amount will be more than the one indicated above.

FINTRAC works with law enforcement agencies and its employees must report for any violation.

Punishment can be not only administrative but also criminal. If company representatives:

- did not report a suspicious transaction: up to CAD 2 million and/or imprisonment for five years;
- did not report a large transfer of money: up to CAD 500,000 (1 violation), 1 million (for the second and further);
- do not keep the necessary documentation: up to CAD 500,000 and/or five years in prison;
- do not help law enforcement agencies: up to CAD 500,000 and/or imprisonment for five years;
- disseminated data on a suspicious transaction to third parties: up to two years in prison.

If an employee reports to their manager for suspicious transactions, they will not be penalized.

1.5 Signs of suspicious transactions or high-risk leads

There are numerous generic and industry-specific signaling devices that help determine the relationship of a transaction to terrorist financing. Below we have provided examples of them. If a transaction includes one or more of these factors, it is suspicious. An employee of the company should study it and, if necessary, inform FINTRAC.

Common Factors

This section contains common indicators that can help you identify a suspicious transaction. The operation must include various of these factors. Alone, they are considered normal for some transactions.

An employee should be alert if a client:

- says he is involved in money laundering;
- refuses to provide the necessary information about his identity and the origin of money;
- provides information that is not truthful or unverifiable;
- opened accounts in several banks in the same province but had no apparent reason;
- uses the same address many times, but changes the first or last name;
- asks about internal control;
- does not tell anything about the purpose of the transaction;
- asks for information that is not related to a financial transaction;
- engages in unusual activities;
- knows nothing about the purpose of the transaction;
- knows a lot about money laundering;
- visits a high-risk country several times a year.

Industry signaling devices

An employee should be alert if a client:

- wants to conduct transactions at the wrong exchange rate;
- asks to pay a commission for the transfer, which is higher than the stated one;
- asks for banknotes of the largest denomination;
- cannot provide information about the payee;
- does not want to provide information about the payee or requests a bearer transfer;
- wants the transfer to be made not by check, but in cash;
- converts cash into a check, although that doesn't make sense;
- exchanges cash for small money orders to several senders;
- wants to make an exchange of funds in an unusual place;
- says that the transfer should be received by a third party;
- buys a lot of traveler's checks, but is not going to go anywhere;
- makes a lot of money transfers;
- buys many checks for small amounts for different names;
- asks to write a check or make a money transfer to bearer;
- exchanges a lot of foreign currency, but for another foreign currency;
- orders a lot of money transfers and changes the type of payment on each one.

This is not a complete list of factors. You can find all of them here:

https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/msb_mltf-eng

Part B – Appointment of a Compliance Officer

A Compliance Officer is the person who is appointed to ensure the Company's compliance with the AML/CFT requirements.

Their responsibilities include:

- Implementing customer identification requirements.
- Implementing procedures for record keeping requirements.

- Making officers aware of laws relating to AML/TF and, train officers, employees and agents to recognize suspicious transactions.
- Checking all persons before hiring them as employees.
- Assessing and periodically updating overall AML/TF risk of the Company;
- Reporting to FINTRAC;
- Reporting periodically to the board of directors/senior management/owner.

The Compliance Officer is required to:

- have the power and the resources needed for discharging their responsibilities effectively.
- have a deep knowledge of AML/CTF requirements and of the practice and client base to be capable to deal with risks.

The Compliance Officer may entrust certain responsibilities to other employees however the Compliance officer retains the duty for the implementation and execution of the compliance program.

Part C Policies and procedures

This policy sets out the responsibilities of the people who carry out the identification of the transactions to be reported. There are also guidelines for staff who keep records and identify themselves.

1.1 Registration in the FINTRAC electronic reporting system

The employee must register the Company in the electronic system FINTRAC, F2R, or make sure that the company is already in the database. So the employee will be able to provide electronic reporting on time and in full.
After registering on FINTRAC, the company receives a unique code that must be included in each report. The number should be retained by a Compliance Officer. He submits all reports to FINTRAC and is responsible for their accuracy.
To register, use the following contacts:

- https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng;
- phone: 1-866-346-8722 (calls are free);
- Address: Financial Transactions and Reports Analysis Centre of Canada 234 Laurier Avenue West, 24th floor Ottawa ON K1P 1H7 Canada

1.2 Suspicious Transaction Reporting and Record-Keeping Policies

This section explains what suspicious transactions are. These are financial transactions that may be related to money laundering or terrorist financing. The company must reasonably suspect them. Employees are required to report to FINTRAC of each such transaction. The information should come immediately after the completion or attempted execution of such a suspicious transaction. But before that, the Company is obliged to take all possible measures that will establish reasonable grounds for suspicion. There is no minimum amount threshold.
The company must:
● check a suspicious transaction;
● evaluate the facts and context of the suspicious transaction;
● link ML/TF indicators to the assessment of all facts;
● explain the grounds for suspicion (formulate the facts, context, and ML/TF indicators that will give rise to the suspicion).
Now let's look at the concept of «communicate as soon as possible». It means that the Company has already taken all measures that helped determine the reasonableness of the suspicions. The development and presentation of such open-source software are considered a priority.
Employees should immediately report transactions that they consider suspicious. The information is provided to the head of compliance in writing. He (she) forwards this report to FINTRAC and informs the management about it. Copies of all correspondence with FINTRAC must be kept in a safe.
The law states that STRs must be sent electronically. If it is not technically possible, the report can be sent in paper form.
There are two options for reporting by e-mail and can provide secure encrypted data transmission. Such methods will guarantee the confidentiality and integrity of all information:
● FINTRAC web reports: https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng
● Batch file transfer: https: //www.fintrac-canafe.gc.ca/reporting-declaration/Info/batch-lots-eng#how

Confidentiality and immunity

The Company is restricted to notifying any person, including the client, about making an STR. This is relevant regardless of whether or not such an examination has started.

The Company should not ask for any provisions of information from the client performing the transaction that it would not typically ask for during a transaction.

The Company may bring no criminal, civil, administrative, or disciplinary proceedings against individuals to make a report concerning a suspicious transaction in good faith.

Contents of an STR

An STR should encompass the following aspects:

- Details about the participants;
- The place and time of completion/attempt of financial operation and the reason of its non-completion if happened;
- Financial instruments utilized during the operation;
- Whether the transaction has any connection with the assignment or attempt of an ML/TF offense.

The Company should keep a duplicate of an STR for at least 5 years from the date of submission.

1.3 Reporting on significant cash transaction reports (SCTRs) and record-keeping policy

Regulations: If an MSB receives CAD 10,000 or more in cash, non-regardless of the amount of transactions within 24 hours, it must inform the regulatory body within 15 calendar days.

Policy: CruisePay does not accept cash, and thus, will not need to submit an SCTR or keep records. For clients offering to provide cash for the payment, alternative payment options will be provided.

In case of accepting cash in error, the Compliance Officer must:

- Provide SCTR within 15 calendar days of conducting of financial operation.
- Create and hold an SCTR.
- Hold a copy of the SCTRs in a secure place.

Information that must be described in an SCTR can be found in FINTRAC's Guideline 7A Submitting significant cash transactions reports to FINTRAC Electronically and Guideline 7B7 Submitting Large Cash Transaction Reports to FINTRAC by Paper.

SCTRs must be retained for at least 5 years from the date of creation.

1.4 Terrorist property reports (TPRs)

Regulation - In case of property in the Company's possession or control that belongs to a terrorist organization, the Compliance officer must report to FINTRAC immediately.

Two situations can cause the necessity to submit a TPR to FINTRAC:

1) Reasonable assurance that property is under ownership or control of a terrorist organization.
2) Belief that property belongs to a person or organization that is believed to be guilty for:
   - having been involved in terrorist activities; or
   - operating as a representative of or in partnership with any person or organization performing any of the activities as mentioned earlier.

Policy: the clients are checked against lists daily, and transactions are checked against lists and ML/TF indicators.

All cases of terrorist property in the Company's possession or control are delivered to the Compliance Officer. If such circumstances arise, the Compliance officer must prepare a report to FINTRAC and inform the RCMP (unclassified fax: (613) 825-7030) and CSIS Financing Unit (unclassified fax: (613) 369-2303). TPRs must be sent in paper format to

FINTRAC. Preparing a report, the Compliance officer operates under FINTRAC's Guideline 5 Submitting terrorist property reports.

1.5 Electronic funds transfer reports (EFT)

The Company is required to inform about international EFTs that total or exceed CAD 10,000 to FINTRAC during 5 working days after the transfer of the non-SWIFT or standardized SWIFT payment messages. These messages are delivered in 2 ways: in a one transaction or in a series of transfers of less than CAD 10,000 each (that totally account for CAD 10,000 or more) in the 24-hour rule case that signifies that the Company is aware of the financial operations that were made within the period of 24 hours by the same client.

The 24-hour-rule will not have any effect on any of the amounts under CAD 10,000 included in an EFT with more than one beneficiary if sent to a public body, a large corporation, or the administrator of a pension fund, regulated on a federal or provincial level.

Under the policy of the Company, transactions are checked daily. The Compliance Officer is responsible for sending SWIFT EFT Reports and non-SWIFT EFT Reports to FINTRAC during 5 working days after the transfer. The day of the transfer means:

- The day the instructions were transferred to the Company;
- The day the Company transfers the instructions regarding the transfer of funds.

When an EFT report should be prepared, the Compliance officer acts under to the following FINTRAC's Guidelines: Guideline 8A8, Guideline 8B9, and Guideline 8C10.

Section 2 – Client information record keeping

2.1 – Overview

Record keeping is an essential aspect of being professional and accountable for the services that money service businesses provide to clients. Establishing business relations and account opening, the Company must record all client information accurately and timely. It may include but is not limited to personal details; name, date of birth, and contact details, including address, occupation, employment, tax residency, source of wealth, purpose and planned use of the products and services, third party involvement, etc.

For legal entities, the information on the beneficial owners of the entity and those who control the entity is required, as laid down in FINTRAC guidance11 and described below.

2.2 – Recording client information

According to the policy of the Company, recording of client information applies to all clients who have a business relationship with the Company.

The Company confirms its compliance with the requirement to create a client information record by filling client applications for payments products and services, including required information. Details in client information records differ subject to the type of client (individual or entity) and the nature and/or volume of the client's financial operations. A report should contain the following information:f

- Client's identifying data (individuals and entities)
- Industry and profession (business type for entities)
- Beneficial ownership details (entities)
- Third-party determination and information
- Politically exposed person determination
- Purpose and planned use of the products and services

More information on what must be included in the client information record is stipulated in Section 2.3.

2.3 - Summary chart

Components of a client information record	*Case of need*	*Information required to be recorded/kept*
Client information for individuals – Recorded on applications and forms.	If the client is setting up a business relationship with the Company or for occasional transaction.	Client information: ● Name ● Address ● Date of birth ● Industry and profession (descriptive) Client identification details: ● Identification details to include details of type, identifying number, place of issue, expiry. * Details of required information are laid down in Section 3 "Client identity"
Client information and beneficial ownership and control records for entities – Recorded on applications, forms and copies retained of supporting documentation from the client. * The definitions, additional policy and procedure information are laid down below.	If the client is setting up a business relationship with the Company or for occasional transaction.	Client information for all types of business entities: ● Name ● Address ● Incorporation or other identifying number ● Jurisdiction ● Detailed description of the entity's principal business and industry ● Signatory information to include name, address, DOB, profession, identification [including details of type, identifying number, place of issue, expiry. Information that confirms existence of a business entity and beneficial ownership, structure and control information: ● Duplicates of documents used to confirm existence that include: O Certificate of corporate status (corporations) o Notice of assessment issued by municipal, provincial, territorial or federal government (corporations)

		o Partnership agreement (entity other than a corporation) o Articles of association (entity other than a corporation) ● Duplicates of records obtained to confirm information about the individuals who ultimately control the entity, ownership and provisions relating to power to bind such as: o Articles of incorporation/association o Shareholder or partnership agreements o Annual return (T1 Sch50 or equivalent) o Bylaws of the corporation o Certificate of incumbency o Trust deed o Evidence of power to bind ● Names of all directors (for corporations) ● Names and addresses of trustees, known beneficiaries and settlors of the trust (for trusts) ● Names and addresses of all individuals/entities who directly or indirectly own or control 25% or more of the entity (for entities other than trusts) ● Information establishing the ownership, control and structure of the entity. If this information cannot be obtained or accuracy not confirmed record: ● Name of the most senior managing officer of the entity and ascertain their identity and treat the client as high risk Not-for-profit organization requirements Determine whether or not the entity is a registered charity for income tax purposes. If it's not a registered charity, determine

		whether or not it solicits charitable financial donations from the public.
Third Party information determination – Recorded on applications and forms. * The definitions, additional policy and procedure information are laid down below.	If the client is setting up a business relationship with the Company or for occasional transaction.	● The Company should define whether there is a third party involved with interest or control of the conduct of an activity or financial transaction on their behalf. If yes, the following information about third party is collected: ● Name and address ● Profession or principal business ● Date of birth (if an individual) ● Incorporation number and place of incorporation (if a corporation) ● Nature of relationship between third party and client If connection with a third party is suspected even though the client has stated there is not a third party involved, document why we suspect the individual is acting on a third party's instructions.
Politically exposed person (PEP) or Head of an International organization (HIO) determination – Recorded on applications and forms. * The definitions, additional policy and procedure information are laid down below.	If the client is setting up a business relationship with the Company or for occasional transaction.	● The Company should define whether is client a PEP or HIO (includes close relatives/close associates)? If yes, the Company collects the following information about a PEP or HIO: ● The name, relationship and office/position; ● The source of the funds, if known, that were used for the transaction; ● The date we determined the individual to be a PEP or HIO; ● The name of the member of senior management who reviewed the transaction; ● The date the transaction was reviewed

Business relationship information – Recorded on applications and forms. * The definitions, additional policy and procedure information are laid down below.	If the client is setting up a business relationship with the Company or for occasional transaction.	Record of the purpose and planned nature of the business relationship on applications and forms (for instance, foreign exchange for travel or purchase of goods, funds transfers for family support or purchase of goods, etc.)

a) Beneficial ownership and control records

Under beneficial ownership is meant the identity of the individuals who ultimately own or control more than 25% of a company's shares or rights. Since this type of ownership may be either direct or indirect, the indirect ownership reference is essential. It may require additional documentation to ensure that disclosure of these individuals has been reached.

According to the Company's policy, reasonable measures must be undertaken to confirm and keep records of the information about the entity's beneficial owners while confirming the existence of an entity. All information must be documented on applications and forms. Duplicates of all documentation used to obtain/ensure beneficial ownership and control (mentioned in the table above) are kept in the client file. Details on confirming the existence of entities are available in Section 3, "Client identification" of this program.

To determine beneficial ownership, the Compliance Officer must research as many levels of information as necessary, not to miss any details. Nevertheless, there may be cases where no person owns or controls 25% or more of an entity. Non-regardless of obtained outcomes, the Compliance Officer must keep a record of the information received.

Reasonable steps to verify the accuracy of beneficial ownership information would include requesting the client submit appropriate documentation or refer to publicly available records as described in the chart in Section 2.3 of this program. All documents obtained to verify the information or the public source, for instance, the website where the Compliance officer detected the data, should be kept in the Company's records.

There is no need to determine the identity of the most senior managing officer when there is no person who owns or controls 25% or more of an entity. Nevertheless, the Compliance officer records the names of persons who take a managerial role or own a percentage of shares that the Compliance officer determines to be substantial (e.g., 10%), even if it is less than 25%.

Suppose the client refuses to submit the information about beneficial ownership when a beneficial owner exists. In that case, such an individual must be deemed a high-risk client, and additional identification of the most senior managing officer is required. It may also lead to a breach of doing business with this client without providing this information.

Information about ownership, control, and structure are available in FINTRAC's Guidance12: Know your client - Beneficial ownership requirements - Appendices.

b) Third party determination and records

A third party can be defined as a person or entity who gives instructions to another person or entity to carry out an activity or financial operations on their behalf. When ascertaining whether a third party is engaged, it is not about who owns or enjoys the benefits from the money or who

is conducting the operation, but rather about who instructs to manage the money or complete a transaction or activity. Aiming to identify who the third party is, the Company should consider whether the individual is acting on someone else's instructions. If so, that someone else is determined as the third party.

According to the Company's policy, the Company always asks the client to disclose if a third party exists.

How to make a third-party determination?

At the time of application, the client is requested whether any other person or entity will have access to or manage the account or use payment services or products, or whether another person is giving instructions referring to account opening, payment services, or products? The client's answer is documented on applications and forms. If there is a third party engaged in the operation, the following information about the third party is also recorded on applications and forms such as:

- Name and address;
- Profession or principal business;
- Date of birth (if an individual)
- Incorporation number and place of registration (if a corporation);
- Nature of relationship between third party and client

When the Company suspects that there is a third party engaged, the Company keeps a record, on application and forms, to indicate the following:

During the establishment of a business relationship or the occasional transaction whether, according to the client, the transaction is being carried out on behalf of a third party.

c) Politically exposed persons (PEP) or Head of international organization (HIO) identification and records

A PEP is an individual who is or has been given a prominent public function, occupying one of the following offices or positions subject to specific terms and expiry below-mentioned:

- Legislative bodies;
- Executive bodies;
- Diplomatic roles;
- Judiciary bodies;
- State-owned enterprises;
- Also, this list includes heads of international organizations:
- Central financial institutions,
- Armed forces
- International sports committees

(Examples are available in FINTRAC guidelines13).

A PEP also refers to the relatives and close associates (either personal or business relations) and as:

- Parents,
- Children,
- Spouse or partner,
- Siblings,

- Indirect family members (such as in-laws).

Terms and expiry

Nonresidents – if the person takes up or has ever taken the post (including deceased).

Residents – if the person takes up or has taken the post in the past 5 years.

HIO – if the person currently occupies a post.

According to the Company's policy, the Compliance Officer must define whether a person who asks to set up a business relationship or to make an EFT in amount CAD 100,000 or more during an occasional transaction, or a person who receives an EFT accounting for CAD 100,000 or more is a foreign or local PEP, an HIO, or a relative or close associate of any of these. The Company verifies whether it is servicing an individual in this status within 30 days after the transaction is made.

Suppose it was defined that the client is a PEP; setting up the business relationship or financial operation must be either approved or rejected by the senior management. Since such clients are considered high-risk, the appropriate special measures must be applied. These measures encompass:

1. Determination of the source of client's or transaction's funds;
2. Approval of the business relationship or transaction by the senior management;
3. Recording all of the measures taken for the determination, review, approval, and screening.

How to identify a PEP/HIO?

The Company requests the client whether they have a status of a PEP; their "yes" or "no" answer is recorded in client applications and forms. The Compliance officer may also seek information from a credible source of commercially or publicly available information about PEPs. Suppose the client is a PEP, the Compliance officer should file the following information about a PEP:

- The office/position.
- The source of the funds used for the financial operation.
- The date of the transaction review.
- The date the Company determined the person to be a PEP.

How often should a PEP/HIO identification be made?

Once identified that a person has a PEP/HIO status, the Company will not renew this operation. However, if initially identified that a person was not a PEP/HIO, the Company must still implement practical actions (screening of PEP/HIO lists against client's database regularly) to identify whether we are providing services for a PEP/HIO during a business relationship, since the client may acquire another status.

d) Reports of a business relationship

Business relationships are the connections between the client and the Company once a client's account is opened. If there is no account, a business relationship is set up when a client has performed 2 or more transactions or activities through the Company, for which identity verification is required.

According to the Company's policy, the Company creates a business relationship with all clients who open accounts and records the purpose and planned use of the account, payment services, and products. This operation should be done within 30 calendar days after the 2nd transaction or activity. If occasional transactions are performed, the Company should define whether a business relationship has been set up immediately after the 2nd transaction or activity. Also, the Compliance Officer should verify the client's identity.

Having established a business relationship, the Compliance Officer is required to complete the following activities:

- record the purpose and planned nature of the business relationship
- do ongoing screening of the Company’s business relationship with a client to:

❖ identifying any suspicious money transfers;
❖ constantly updating the client identification and beneficial ownership information, including the purpose and planned nature records
❖ regularly assessing a client's risk level grounded on their financial operations;
❖ determining if the transactions and activities coincide with information, you have about your client
❖ keeping a record of the actions you take to monitor your business relationships and receive data.

More information about monitoring and updating client information is available in Section 4.3 of this program.

2.4 – Appropriate steps

Appropriate steps are activities the Company implements to meet certain AML/CTF obligations. For instance, the Company must take appropriate steps to verify beneficial ownership information, to identify whether we the client has a status of PEP or HIO, whether the client is instructed by a third party, etc., as described in this program. These activities are documented in this program and other Company's internal documents. The Compliance Officer must record any time the Company takes appropriate steps if the relevant step is unsuccessful.

Appropriate steps must not be confused with and not applied to obligatory data elements.

Documenting appropriate steps

A record is kept when appropriate steps were undertaken but failed. A relevant step is considered unsuccessful when the Company does not receive a "yes" or "no" response and cannot make a conclusive determination. If appropriate steps fail to succeed, the Compliance officer must record the following information:

- The action(s) taken
- The date on which the action(s) was taken
- The reason why the action(s) was unsuccessful

The client's refusal to submit is considered as a part of the overall assessment of client risk.

The records of all appropriate unsuccessful steps should be retained for at least 5 years after they were created.

Section 3 – Verification of client identity

According to law, verification of the identity of an individual and proving the existence of a corporation or other entity under the PCMLTFA and associated regulations must be done by all MSBs.

According to the Client policy, the identity of individuals is verified, and/or the existence of entities is confirmed for all clients.

Details about measures taken/procedures to ascertain the ID of individuals are available in section 3.1 of this program, and details about steps taken/procedures to confirm the existence of entities are laid down in section 3.2 of this program.

3.1 Individuals

Ascertaining the identity of an individual, the Company applies to one of 2 methods.

Single Record Government-issued photo identification(ID) documents method

The Company must review the original, not duplicates of the individual's photo ID in the presence of the client, and conduct a visual comparison with the following documents:

- Passport
- Driver's license
- National identity card
- Permanent resident card
- Or equivalent issued by an authority on the provincial, territorial, or federal levels (not a municipal) that comprises such personal details as photography, full name, address, birth date, and document's expiry date.

The ID document is acceptable if it coincides with the information submitted by an individual and comprises the name, photo, and identifying number. It must be valid and unexpired.

The Company's appointed employee or the Compliance Officer can check the document's validity in person by observing the original in its physical form and its security characteristics in the presence of the individual. The main task is to identify the validity of the document, check whether the issuing body had the power to grant the document and whether it remains valid and unexpired.

When the physical presence is not possible, the authenticity of a document must be identified with the help of technologies that deal with assessing document validity.

If the Company is using the method mentioned above, the Company's appointed employee or the Compliance officer must record the full name as provided on the ID, ID type, ID number, place of issue (jurisdiction), issuing authority and country, verification date and ID expiry date.

Method of Dual Record Verification

This is a more complex approach to data collection that combines a review of original records from 2 different credible resources that the Compliance Officer must consider.

These original records must meet 2 of the following criteria:

- data from a credible resource that encompass personal details such as name and address;
- data from a credible resource that encompass personal details such as name and birth date; or

- data that encompass the name of an individual and approve the existence of a bank account with a financial institution.

This information may be taken from different credible resources (certificates, forms, statements, etc.) and can be submitted through an original form or another version: the document can be scanned, converted to an electronic file, or submitted as fax or photocopy.

Received information must coincide with what the individual submitted. It must come from 2 different sources and can be submitted neither by the individual whose identity is being checked nor by the party carrying out the verification. It is restricted to using one resource for two information kinds to verify the individual's identity.

The Company must record the full name, verification date, the name and type of resources (for instance, bank statements, marriage license); and their identifying number (for instance, account number, certificate number, etc.).

In case of receiving 2 different resources from an aggregator of that information, the tradeline account number or number related to each tradeline must be recorded also.

If the Company fails to complete identification through the documents mentioned above, we must consult FINTRAC's Guidance14.

3.2 Entities

The organization that acts as the subject of any legal relationship is a corporation, trust fund, partnership, or association with unincorporated status. But, corporations work a little differently than other companies.

To confirm that this is a corporation, the Compliance Officer must consult the Registry of Records. This can be:

- confirmation of the status of the corporation;
- an entry from the security's legislation to be filed every year;
- another entry, such as an annual report issued by an independent auditing firm.

It can also be a notification, a letter from the government (municipal, provincial or territorial, as well as federal).

If the entity is not a corporation, the Compliance Officer must provide a record of this. It can be electronic or paper and represent:

- partnership agreement;
- company charter;
- a record that confirms the existence of a legal entity.

The documentation that the firm will use as evidence can be stored in either paper or electronic versions. In the first case, a compliance officer is required to make several copies and put them in a safe. He (she) must also save the electronic record, protecting it with passwords. In the same case, it is necessary to save the registration number of the company and the alphanumeric combination of the type of record and its source. The electronic record must be publicly available. Verbal confirmation, if it was made, for example, by telephone, is not possible. The point is that all records must be saved in text form.

For example, if a Company takes information about the name and address of a corporation, it can get the names of directors from the federal Corporation Canada database available on the Industry Canada website (http://www.ic.gc.ca). Also, its employees can use various public sources to find registered firms.

3.3 Restrictions on the use of personal information

Using personal information in commercial activities in Canada without the permission of the copyright holder. Such things are protected by the Law on the Protection of Personal Information and Electronic Documents (PIPEDA15). There is issued a specific addition to this legislation in each province. Therefore, any company, when collecting personal data, must inform clients about it. But it is not necessary to report there when their personal information is included in the reports to FINTRAC.

There are questions and answers regarding this legislation on the Government of Canada website. Prepared by the office of the country's confidentiality commissioner to clarify the responsibilities of each side in order to protect their rights by federal laws.

Section 4 — Risk Based Approach

4.1 — Risk Assessment

If we consider the concept of risk, we can read its definition, which is written in the law. This is the probability of an event and its consequences. In jurisprudence, the risk is seen as a combination of the likelihood of something that can happen and the miscalculation of the damage resulting from it. Considering the context of money laundering or terrorist financing, this concept is divided into the national level and the company level. In the first case, these are threats that undermine the integrity of the country's financial system and the security of the entire population. At the company level, it’s the same thing, only at the local level.

Threats can come from a person or a group. That is an object that can cause harm. They are often criminals, accomplices, or terrorist organizations.

Companies or their weak points are vulnerable after these threats. Firms may offer products or services that have a high level of risk.

The impact of a particular risk is measured by the severity of the damage.

Also, we should not forget about the concept of risk assessment. It is an analysis of threats and vulnerabilities that can be used to launder money or finance terrorism. If you are interested in additional details, we recommend looking at the FINTRAC website in the MSB1 risks section.

Types of risk assessments

In order to understand how vulnerable a company will be after certain threats, it is necessary to conduct a risk assessment. The employees of the firm should divide it into two parts:

- analysis of products, services, and geographic location;
- monitoring of relationships, that is, the products or services that customers use, their geographic location, the pattern of transactions.

All this should be reviewed by the company's employees every two years. If any of the key factors change, the review must occur immediately.

If a firm is assessing risk, it must consider products, the geography of customers, and business relationships. Factors vary depending on the scope of the enterprise.

Products and Services

A specific list of products means a higher level of risk. This category includes goods that allow the customer to participate in high-risk transactions. These are products used for money laundering. Most often, this includes goods for which it is very easy to withdraw funds or make transfers. Also, laundering is facilitated by third parties who make a transaction using the product.

Delivery channel risk refers to the medium that is used to simply get a product or service, but most regularly money. If it is possible to receive the goods without personal presence, this is a very high risk, since it is almost impossible to establish the identity of the recipient.

Geographic Risk
Geographic location also significantly affects the overall risk of a company. A higher level is determined if the firm:

- is located close to a region with a high crime rate;
- is associated with clients from high-risk countries;
- is located in a large urban area, as its clients are frequently unknown.

Other factors
Of course, for each company, there are factors that depend on the field of activity. But the operating structure of the business model should be noted separately. We are talking about the number of employees, staff turnover, the availability of technologies that affect the industry.

In order to conduct an objective analysis and assess how your company is exposed to a risk factor, we recommend that you subscribe to the FINTRAC newsletter and read the 18 FINTRAC manual.

How the risks of individual clients are assessed (initial and current)

Each client needs to be assigned a risk rating. If it is high, the revaluation will have to be done on an ongoing basis. Typically, customer relationships are divided into three risk groups, a, b, and c, in ascending order, respectively.

Each client needs to be perceived as a low-risk partner. High risk includes:

- persons holding government positions;
- clients already coming to the attention of law enforcement agencies during suspicious transactions;
- identified terrorists;
- clients who are unable to provide beneficial ownership information.

Any of these factors will be sufficient to transfer the client from group A to group C. In the event that there are three or more points, the partner will default to a high level of risk. If we consider the characteristics of the client, product, service, and delivery, it is worth highlighting the following as a high level of risk:

- heads of international organizations and their closest associates;
- clients who do not have confirmation of the legality of funds;
- orders for large transfers to other countries, which are characterized by a high level of risk;
- involvement of third parties, whose presence should not be in this transaction;
- partners who are in high-risk positions. We are talking about offshore business or online gambling;
- business structures with a complex organization;
- customers with no personal identification, unless there is a valid reason.

Geographic factors are:

- the location of the client outside the local area;
- the partner's residence in a criminal area;
- the firm's ties to companies from high-risk countries.

Other high-risk identifiers include transaction volumes or complexity that do not match customer activity. It is also worth analyzing the cost of his contributions and transfers. If they do not match

the source of funds, you may begin to suspect your partner of illegal activities. The same applies to firms that are listed in part A of this provision.

All customer assessments must be documented using an appendix to this provision. To demonstrate how the company works, you need to keep all copies of them.

4.2 - Risk Mitigation

If a high risk has been identified through a company assessment, mitigation measures should be developed and implemented immediately. An indicative list of them is provided in sections 4.4 and 4.5 of this policy.

4.3 - Ongoing monitoring and updating of customer information

Once a company has established a business relationship with a specific customer, it must continuously:

1. Monitor it.
2. Constantly draw up information about him.

Monitoring and updating of data are carried out in order to:

1. Detect suspicious transactions in time.
2. Assess the level of risk.
3. Determine the correspondence of the transaction to the information that the company already has.

When it comes to an individual, current monitoring should include checking:

- name;
- addresses;
- occupation.

When a legal entity acts as a client, information about:

- name;
- address;
- main activity;
- directors and trustees;
- beneficial ownership.

Beneficial ownership information includes details of the individuals who own the organization.

The law specifies the frequency with which compliance officers are required to monitor customers and partners. It will depend on the risk rating. If a client has a high level of risk, it needs to be checked much more often. Low and mid-level partners' transactions should only be tracked at the time they are made.

Data can be confirmed periodically during ongoing interactions. For example, when a customer posts a business transaction or transaction.

If the client has a high level of risk, his transactions are assessed at the time of their implementation and at the time of early verification. Moreover, the monitoring of this company is saved in a special file and protected by the company's employees.

Customer information should be updated once a year or more often. Its relevance is specified during the call. In order to confirm it, company employees may resort to additional measures. These include reasonable actions and procedures, both in-person and remotely.

4.4 Business based risk assessment

This sub-section provides a list of areas where the Company may have vulnerabilities exploited by offenders with purpose of money laundering or terrorist financing. Here considered are the products and services offered by the Company, way of delivery of products and services and the location of business. The list is not complete and must be updated if any additional risks are identified. For all factors marked as "high-risk", risk mitigation measures must be developed.

FACTORS *Identification of all the factors that refer to the Company and their indication of frequency.*	Current risk level *Assessment of level of raw or untreated risk*	Grounds *Explanation the reason of risk rating assignation.*	*Description of measures that will be applied to mitigate the ML and TF risk.*
Products and services			
Electronic funds transfers ✓ Regularly ___ Often ___ Rarely/Never	HIGH	This type of service can be completed in a non-face-to-face mode, thus posing a risk for MK and TF. Also, large amounts of money can be transferred outside/to of Canada, which can hide the source of the capital.	• Enhance the frequency of EFT transaction monitoring to make certain that they are checked against the client profile and that any transactions of suspicious nature have been estimated and reported to FINTRAC; • Limit certain ETFs; • Look for additional information that will help to ascertain the identity of the client or beneficial owners; • Verify the origin of funds for all clients; • Train employees to guarantee the deep knowledge of the products offered and the

			ML/TF risk that is connected with the offerings and related transactions.
Digital wallets _✓_ Regularly ___ Often ___ Rarely/Never	HIGH	Ability to save money, simplicity of withdrawals and option to transmit money more fast or anonymously.	This option is available only to clients who passed identification. The measures of the Company will include: • Verification of origin of money for all clients; • Limit certain transactions; • Ongoing monitoring; • Non-acceptance of cash for deposits; • Training employees to guarantee the deep knowledge of the products offered and the ML/TF risk that is connected with the offerings and related transactions.
Products provided with the help of middlemen (intermediaries or agents) ___Regularly ___ Often _✓_ Rarely/Never	HIGH	the use of third parties may increase the Company's inherent risks as they may not be accountable to AML/ATF laws or be supervised in an adequate way.	The Company does not provide products and services through the third parties.
Digital money/wallets ___Regularly _✓_ Often ___Rarely/Never	HIGH	New payment modes can be used to make a transaction more quickly and/or anonymously.	This option is available only to clients who passed identification. The measures of the Company will include:

			• Verification of origin of money for all clients; • Limit certain transactions; • Ongoing monitoring; • Non-acceptance of cash for deposits; • Training employees to guarantee the deep knowledge of the products offered and the ML/TF risk that is connected with the offerings and related transactions.
Delivery modes			
Face-to-Face (on-boarding and ongoing transactions) ___Regularly ___Often ___Rarely/Never	LOW		Given the low level of risk, no measures are needed.
Non-face-to-face (through telephone, e-mail, Skype, or other means.) _✓_ Regularly ___ Often ___ Rarely/Never	HIGH	Verification of clients the physical presence of which is not possible poses higher risk as it is more complicated to get know who the client is and who the Company is transacting with.	• Leverage technologies that deal with assessing the validity of documents, or • Negotiate the meeting with the client in person before performing 2 transactions that follow ID document; • Not provide services to new clients if they refuse to meet without a

			justifiable reason.
Geography			
Vancouver ✓ Regularly ___ Often ___ Rarely/Never	MEDIUM	Since Vancouver is a medium-crime location, the risk that money may come from illegal sources is reduced.	• Verify the origin of money for all clients. • Regularly review information about crime from credible sources that is available in Internet. • If needed, train employees to make certain they know the the situation with crimes in the Company's area and refresh their memory of due diligence at on-boarding such as occupation and source of funds.
Connections to countries, marked as of being high-risk (transactions from countries that may constitute a ML/TF risk.) ___Regularly ✓ Often ___Rarely/Never	HIGH	Transactions to/from foreign jurisdictions present a higher level of ML/TF risk.	• Verify the origin of money for all clients. • Update the list of prohibited jurisdictions. • Estimate again the level of risk associated with the client as transactions is in progress. • Review the sanctioned countries listing regularly (annually) or as informed of amendments to

			the listing through FINTRAC. It can be found on the Office of the Superintendent of Financial Institutions' website (http://www.osfi- bsif.gc.ca)
Other risk factors			
These may include employment retention, consistent geographical location, number of employees, etc. ✓ Reflects the Company current practice __ Does not reflect the Company current practice	LOW	Low number of employees and/or high employee retention, single office location with some changes in geography, products or client base.	Given the low level of risk, no measures are needed.

4.5 – Relationship based risk assessment

Business relationships *(Identification of business relationships clients marked as "high-risk" and estimation the level of risk)*	Grounds *Explanation the reason of assigning a certain rating*	Increased measures to verify ID for relationships marked as "high-risk"	Mitigation measures for relationships marked as "high-risk"	Description of measures undertook to keep client information relevant for relationships marked as "high-risk"	Increased monitoring for relationships marked as "high-risk"
Group A - LOW	The volume, timing, complexity of client's transactions face-to-face matches the purpose of the business relationship/account and not pose any automatic high risks.	N/A	N/A	Update client information regularly (annually) and when is required (e.g., personal data has been changed)	Monitoring on regular basis transactions and business relationship for low risk

Group B - MEDIUM	The volume, timing, complexity of client's transactions non-face-to-face matches the purpose of the business relationship/account and not pose any automatic high risks.	Determine the validity of a government-issued ID document with the help of appropriate technologies.	N/A	Update client information regularly (once in 10 months) and when is required (e.g., personal data has been changed)	Monitoring on regular basis transactions and business relationship for medium risk
Group C - HIGH	Client for whom STRs have been already provided due to the existence of reasonable grounds	Ensure a valid document with photo ID issued by a federal or provincial government that is provided by a client is ascertained.	• Approve business relationships with senior management. • Establish maximal limits for transactions according to client profile. • Ask for explanation of origin of client's funds.	Update client information regularly (once in 9 months) and when is required (e.g., personal data has been changed).	Check each transaction that is performed by a client that pose high risk as the time it is conducted. Take and keep brief records in which the review of the transactions is described. Assess transaction against the client's profile. Ask for additional information if the volume, timing, complexity of client's transactions face-to-face does not match the purpose of the business relationship/account.
	PEP as this client may be engaged in ML/TF other financial crimes due to their power	Ensure a valid document with photo ID issued by a federal or provincial	Approve business relationships with senior management.	Update client information regularly (once in 6 months) and when is required	Monitor transactions and business relations. Regular review of client's transactions.

		government that is provided by a client is ascertained.		(e.g., personal data has been changed).	
	Client who refuses to submit information about beneficial ownership as this may mean that the client wants to conceal these relations.	Ensure a valid document with photo ID issued by a federal or provincial government that is provided by a client is ascertained.	Report about suspicious actions of a client and do not set up business relations with such a client.	N/A	N/A
	High-risk clients that have potential triggers at onboarding or as indicated during ongoing monitoring that have been estimated as posing high risk. These triggers are described in the risk assessment tool (Appendix).	Ensure a valid document with photo ID issued by a federal or provincial government that is provided by a client is ascertained.	Approve business relationships with senior management.	Update client information regularly (once in 6 months) and when is required (e.g., personal data has been changed).	Check each transaction that is performed by a client that pose high risk as the time it is conducted. Take and keep brief records in which the review of the transactions is described. Assess transaction against the client's profile. Ask for additional information if the volume, timing, complexity of client's transactions face-to-face does not match the purpose of the business relationship/account. If necessary, look for additional information about the client. Measures that will trigger early warning signals and require a

					mandatory review have to be enhanced.

Section 5 - Timing of records

In order to comply with company documentation requirements, employees must maintain legible records. This is done in order to provide all necessary information to FINTRAC within a maximum of 30 days after the request is received. Sometimes the documentation is required in court or law enforcement agencies are interested in it. This is often done in order to counter money laundering organizations. The firm must keep all records or their copies electronically. The hard copy is also allowed but in some cases.

The firm must have recorded:

1. All reports.
2. Large monetary transactions.
3. Transfers in the amount of CAD 3,000 or more (if the company receives this money through traveler's checks or transfers).
4. Transfers for CAD 1,000.
5. Currency exchange

Law enforcement agencies may also require records of various actions, agreements, preventive measures for money laundering and terrorism, an internal memorandum.

The firm must keep records for 5 years about:

- individual identification of the client;
- the existence of a certain object;
- beneficial ownership.

It also includes protocols for identifying individuals deemed to be politically significant for the country and documentation from overseas organizations.

The firm must keep records of suspicious transactions, large money transfers, and records of real estate owned by terrorists in a safe place. Their shelf life is at least 5 years. Other documents are kept for more than 5 years.

Part D — Ongoing Training Program

For individuals who interact with customers, see or process their transactions, are responsible for their funds, specialized training should be provided. Its frequency is not indicated directly in the legislation. But it is known that this is an ongoing process that is mandatory for all new employees. AML/CTF update training must be completed every year. It depends solely on changes in legislation and new products with which the company begins to cooperate.

The training consists of the information in Sections A and C. The optional curriculum includes modules taught by the Compliance staff or external consultants invited by management. All changes are recorded in the table below.

Specially appointed employees are responsible for training, its requirements and information base. Course records must be kept.

Training completion tracking

Employee (Name/Surname)	Type of training and content (initial training, review of policies, procedures and background information, module provided by insurer, etc.)	Date	Employee signiture
	Initial training, review of policies, procedures and background information	August 28, 2023	

Part E – Approval and adoption of policies, procedures and training program

The policies, procedures and training program documented in this Compliance program have been approved and adopted by the Director of CruisePay ltd.

Date this program was adopted: August 28, 2023

Part F — Program Review

When it comes to policies, they need to be reviewed every year. This is done by a Compliance Officer. If there are any changes in the company at the official level, the policy review should be carried out immediately. We are talking about restructuring the business, making changes to the regulatory framework, opening a new office. After the completion of the check, the specialist must sign the documentation for its implementation no later than 30 days later.

Program Review		
Completed by:		Date:
Results reviewed by:		Date:
Compliance item reviewed	Yes/No	Results of testing
1) Appointment of a Compliance Officer		
Testing includes: Ensure a Compliance officer has been appointed and approved by senior management.	Yes	A Compliance officer has been appointed as indicated in the program and the appointment has been approved by the principal as indicated in the Compliance officer section of this program.
2) Approval of written compliance policies and procedures, review of legislative obligations		
Testing includes: a) Certify policies and procedures have been approved by the senior management.	Yes	Policies and procedures have been approved by the Director of the Company as indicated in Part E.
b) Review the FINTRAC website (https://www.fintrac-canafe.gc.ca/publications/pub-eng) to make certain if there are new legislative updates proposed. If there are any, make updates as required to ensure program is up-to-date with FINTRAC guidelines	Yes	The website was reviewed, effective legislative changes adopted as of October 2020 are incorporated in this program.
c) If any reports have been made to FINTRAC, ensure appropriate records have been retained.	N/A	No circumstances arose which rendered reporting to FINTRAC necessary.
d) Review the business-based and relationship-based risk assessments to ensure that all risk categories and factors described in Section 4 have been considered and that assessments accurately reflect	Yes	Risk assessments encompass all categories.

your business and client base.		
e) Review all high risks defined in both assessments to make certain risk mitigation measures have been developed and are efficient.	Yes	Risk mitigation measures have been documented and implemented.
f) Review 10% of high-risk clients to check whether enhanced measures have been conducted i.e., periodic review.	Yes N/A	Reviewed 10% of high-risk clients, evidence of periodic review was noted. OR Currently there are no high-risk clients identified in the practice.
3) Completion of program review and review of results		
Testing includes: a) Certify that a program review has been completed within the last year	N/A	This is the first program documented for the Company; a review will be completed within one year.
b) Certify that the review was signed off by the Director of the Company.	Yes	The results of the review were signed off as indicated above.
4))Ongoing compliance training and review of policies and procedures for the frequency and method of training		
Testing includes: a) Ensure that frequency of training is stipulated in the program.	Yes	According to the training program, training will occur annually
b) Ensure all employees that deal with client transactions are provided with training annually by viewing evidence of training completion.	Yes	Evidence of training in place and reviewed to make certain that all required employees have received training.
Actions required: Currently no actions are required.		
Follow-up actions completed.		

Part G – Revision history

Date	Section changed	Grounds for change
August 28, 2023	N/A	Initial version v.1.0 of the document.

Appendices
Client Risk Assessment Tool

This term is used to document the data of high-risk clients. It is also necessary if there are potential triggers that lead to monitoring.

There are high-risk automatic characteristics. These include clients:

- in a position in politics;
- heads of international organizations;
- that constantly conduct suspicious transactions of
- identified terrorists;
- not providing information about the beneficiaries.

There are also potential factors indicating a high risk for the client. Even one of them may be enough to move a partner from category A to category C. In order for the company to be able to do this, it is necessary to obtain more data, for example, about the products owned by an individual or legal entity, the sources of its funding.

Client characteristics, product, service, delivery channel:

- ❖ large (over CAD 10,000) wire transfers from foreign jurisdictions;
- ❖ involvement of third parties without reasonable grounds;
- ❖ occupation — professions with a high level of risk (for example, business that requires a lot of money, offshore business, business in high-risk countries, online gambling, forex, etc.);
- ❖ the customer's business structure or transactions seem unusually complex;
- ❖ lack of personal identification of the client without a valid reason.

- Geography:

- ❖ the customer is located outside the local or regular customer area;
- ❖ the client lives in a notoriously criminal area;
- ❖ the client conducts offshore business, has connections with countries with a high level of risk.

- Other indicators of suspicious transactions:

- ❖ the volume/timing/complexity of transactions does not match the purpose of the business relationship/account.
- ❖ the cost of deposits/transfers does not correspond to the occupation or source of funds;
- ❖ any indicators of suspicious transactions are identified in the Reference section of Part A.

Document your assessment and rationale here. Notes from ongoing monitoring can also be recorded here.

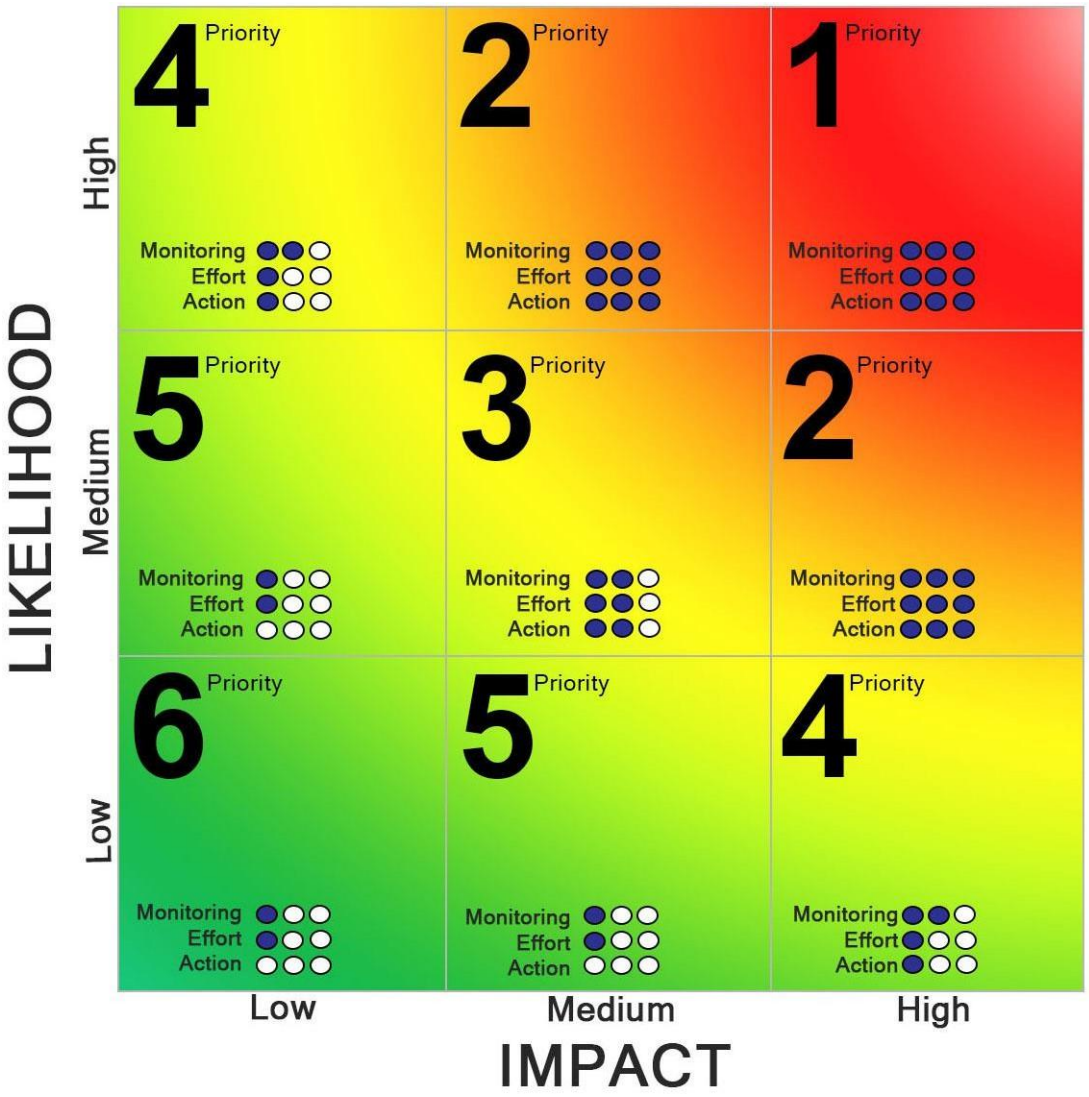
Probability and Severity Risk Matrix

The Company uses the following matrix, when assessing the level of ML/TF risks of its products, services, and clients.

Low risk level	Moderate risk level	High risk level
Stable, well-established client base	Expansion of a client base due to branching, merger, or acquisition	A large and increasing client base, coming from different regions
No electronic transaction services or the website is informational or non-transactional	Electronic transaction services are only started; the Company offers limited products and services	A wide range of electronic transaction services
There are few or no large currency transactions	There is a moderate volume of large currency or structured transactions	There is a significant volume of large currency or structured transactions
Identified are several high-risk clients.	Identified is a moderate number of high-risk clients	Identified is a large number of high-risk clients
Few international accounts or very low volume of currency activity in these accounts	Moderate level of international accounts with unexplained currency activity.	A large number of international accounts with unexplained currency activity
A limited number of fund transfers for clients and non-clients, limited third-party transactions, and absence of foreign funds transfers	A moderate number of fund transfers, several international fund transfers from personal or business accounts to countries marked as "low-risk"	Frequent funds transfers from personal or business accounts to/from high-risk jurisdictions, and financial secrecy institutions
The Company's business is based in a low crime-rated area	The Company's business is based in a moderate crime - rated area	The Company's business is based in a high crime-rated area
No transactions with high-risk geographic locations	Small number of transactions with high-risk geographic locations	Significant volume of transactions with high-risk geographic locations
Low turnover of key AML personnel and frontline personnel	Low turnover of key AML personnel, but changes in frontline personnel	High turnover, particularly, in key AML personnel positions

FINTRAC Risk Assessment Matrix

In addition to the Probability and Severity Risk Matrix, the Company uses the following risk assessment matrix that combines the probability and impact scores of each risk and then ranks them in terms of priority to manage. This is applicable when assessing the level of ML/TR risks of the Company's products, services and clients.



For box #6 no responses, efforts or monitoring are required as both the probability and impact are considered low.

For box #3, allocation of resources for action, effort and monitoring is required. A good practice will be to monitor all business risks/business relations to ensure that the risks do not move into the upper categories.

For box #1, the Company has identified the risks that have high probability and severe impact on business. Thus, anything in this box requires the highest level of resources for action, effort and monitoring.

ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING COMPLIANCE POLICIES AND PROCEDURES

Adopted as of:	August 28, 2023
Revised on:	N/A, initial version of the document
Risk Assessment date:	August 28, 2023
Self-Assessments/Reviews:	N/A, initial version of the document. It is completed every two years.
Signature of the Director:	
Date	August 28, 2023